La profilazione e i suoi rischi

La profilazione e i suoi rischi

Valeria Ferraris

1. Introduzione

Il termine profilazione presenta molti significati e viene usato nel linguaggio comune e in contesti specialisti. Si parla, ad esempio, di profilazione etnica per descrivere una pratica discriminatoria delle forze dell'ordine quando compiono arresti (da ultimi, Delsol e Shiner, 2015) ma profilazione è anche un termine in uso nella psicologia criminale per indicare lo strumento attraverso il quale si individua il profilo del soggetto che potrebbe essersi reso responsabile di un determinato reato di cui si sta investigando.

La profilazione di cui tratta questo scritto è quella definita come "*machine profiling*" (Hildebrandt 2006). Si tratta di quella attività di profilazione svolta dalle macchine sulla base di algoritmi programmati dagli esseri umani, attraverso cui la macchina elabora dei dati e restituisce delle informazioni.

Diversi sono gli studiosi (Marx e Reichman 1984; Clarke 1993; Lee By Grave 2002; da ultima più compiutamente Hildebrandt 2006, 2008a, 2009b) che hanno riflettuto sulla definizione di profilazione e sulle sue caratteristiche ma nonostante questo non esiste una definizione comune. In questo scritto la definizione adottata è quella svilup-

pata precedentemente[1] sulla base dei lavori di Mirelle Hildebrandt: la profilazione è una tecnica di processare automaticamente dati personali e non personali, con lo scopo di sviluppare dai dati conoscenza predittiva sotto forma di profili che possono essere poi applicati per assumere decisioni. Un profilo è un insieme di dati correlati che rappresentano un soggetto (umano, non umano, individuale o collettivo). La costruzione di profili è il processo attraverso cui si rivelano schemi inaspettati all'interno di ampi *dataset* che possono essere usati per creare profili. L'applicazione di profili è il processo di identificare e rappresentare un soggetto specifico o di identificare un soggetto quale membro di un gruppo specifico o di una categoria e sulla base di questa identificazione e rappresentazione di prendere delle decisioni.

In questo capitolo, dopo aver brevemente presentato le caratteristiche e i campi di applicazione della profilazione, si analizzano i principali rischi per i valori e i diritti fondamentali.

2. La profilazione: caratteristiche e campi di applicazione

La profilazione si basa su una tecnica nota come *Knowledge Discovery in Databases* (KDD). Questa tecnica si distingue da altre tecniche di analisi di dati perché "fornisce risposte a domande che non sono state formulate" (Zarsky 2002-2003, 6, traduzione dell'autore). In altri termini fa emergere le informazioni nascoste all'interno dei dati.

KDD è anche denominato *Data Mining*. Quest'ultimo termine risulta però confondente in quanto viene impiegato in letteratura anche per descrivere la mera applicazione degli algoritmi e non l'intero processo. Per questo quando si vorrà indicare l'intero processo si parlerà di *Data Mining* (DM, usando la maiuscola) mentre quando ci si riferisce all'applicazione dell'algoritmo si parla di *data mining*.

Una storica definizione di Data Mining è "*nontrivial process of identifying valid, novel, potentially useful and ultimately understandable patterns in data*" (Fayyad 1996, 6).

La tecnica di KDD o DM si sviluppa attraverso diverse fasi (cfr.

[1] La definizione è stata sviluppata nell'ambito del progetto *Profiling* (http://profiling-project.eu). Una lunga disamina dei molteplici aspetti della definizione di profilazione è stata fatta nel paper "*Defining Profiling*" disponibile all'indirizzo http://papers.ssrn.com/sol3/ papers.cfm?abstract_id=2366564. La definizione è stata successivamente perfezionata nel contributo Bosco, et al. (2015).

Hildebrandt 2008a; Zarsky 2002-2003):

1. La raccolta dei dati.
2. La preparazione dei dati per l'utilizzo (*data warehousing* e *data cleansing*).
3. L'applicazione di algoritmi, il data mining (Hastie, Tibshirani e Friedman 2009).
4. L'esame e l'interpretazione dei risultati.
5. Il follow-up (verifica e correzione).
6. L'applicazione del profilo.

Ciò che qui interessa è il *Data Mining* a fini predittivi che genera nuove informazioni sulla base dei dati raccolti, la fine di "predire dei risultati prima del loro verificarsi" (Zarsky 2011, 292, traduzione dell'autore).

Non necessariamente la procedura è completamente automatizzata. Nella fase di preparazione dei dati, così come in quella di interpretazione e di verifica il ruolo umano può rimanere rilevante. Inoltre può essere l'analista a scegliere quale tecnica di data mining applicare. Tuttavia tanto più la mole di dati si rivela amplia e complessa tanto più difficile risulta garantire un ruolo all'analista all'interno del processo, nonostante gli evidenti ritorni in termini di trasparenza del processo decisionale e di *accountability* che vi sarebbero.

Questo è certamente quanto sta accadendo con i big data e con il loro processo di analisi (*big data analytics*), che può essere indicato come un sinonimo di KDD o DM, ma pone l`accento sulla fonte più che sul processo.

Ogni tipo di dato può essere usato per profilare. Ad esempio i dati relativi ai nostri comportamenti possono essere usati per raggruppare soggetti con comportamenti simili (come fanno oggi i siti di e-commerce con i comportamenti on line); i dati relativi ai nostri spostamenti (facilmente acquisibili tramite un qualsiasi smartphone) possono dire dove siamo stati e quando, ma anche dedurre da questo abitudini, gusti, relazioni con altre persone, etc. Con più sofisticate tecnologie come *smart cameras* e *wearable sensors* possono essere raccolte informazioni sulle nostre caratteristiche biometriche per una gamma ormai sempre più ampia di utilizzi.

Sono infatti molteplici ed in espansione i campi di applicazione delle tecniche di profilazione. Dal settore del cd. *Intelligence Led Policing* (Van Brakel e De Hert 2011-2013; Sanders, Weston e Schott 2015) dove l'approccio è sempre più rivolto alla identificazione e ana-

lisi di rischi prima che questi possano concretizzarsi (Anderson 2010), a quello della *Open Source Intelligence* (OSINT) dove dalla sistematica raccolta e analisi di informazioni pubblicamente disponibili, come quelle sui social, si ricavano informazioni utili a scopo investigativo. Ugualmente ampie applicazioni vi sono nel settore del contrasto al riciclaggio e al finanziamento del terrorismo (Cahnhoto e Backhouse 2007) o dell'evasione fiscale. Lasciando il settore del contrasto alla criminalità, la ricerca in materia di salute vede svilupparsi sempre più la profilazione al fine di analizzare i fattori di rischio e l'efficacia di determinati trattamenti nonché, in generale, la ricerca nel campo della medicina predittiva. Lo stesso dicasi per la ricerca in ingegneria dei trasporti, che elabora dai dati relativi ai nostri spostamenti modelli di mobilità in un'ottica di maggiore sostenibilità (Gianotti e Pedreschi 2008).

3. La profilazione come minaccia ai diritti e valori fondamentali

Come appena sottolineato, la profilazione porta certamente vantaggi ma pone anche seri rischi per il suo impatto su diritti e valori fondamentali. Rischi di discriminazione, sterotipizzazione, diseguaglianza, inaffidabilità e limitatezza del processo decisionale possono seriamente compromettere valori come la democrazia, la *rule of law*, il diritto a non essere discriminati o quello alla protezione dei propri dati personali. Tanto più l'evoluzione della società è accompagnata dall'impiego di metodi di profilazione, quanto più urgente diventa la necessità di affrontare i rischi che essa comporta.

3.1 *La tensione con i valori fondamentali*

La tensione tra democrazia liberale (Zakaria 1997) e profilazione sta nelle caratteristiche stesse di quest'ultima. La profilazione è certamente una tecnica affascinante: rimanda all'idea che gli esseri umani possano raggiungere un livello di conoscenza non prevedibile precedentemente che permetterà di prendere decisioni migliori. Tuttavia esiste un lato oscuro: rende "invisibile tutto ciò che non può essere tradotto in dati leggibili da una macchina" (Gutwirth, Hildebrandt 2010, 33, traduzione dell'autore). Ciò implica che l'intero processo decisionale potrebbe essere viziato da una incompleta raccolta di dati

iniziale, a cui l'essere umano non riesce a porre rimedio nel momento in cui gli algoritmi applicati diventano così complessi da far perdere di vista l'errore iniziale.

Inoltre, scarse sono le possibilità per il cittadino di conoscere le ragioni che hanno portato ad una certa decisione ed eventualmente contestarla. Più probabilmente il cittadino conoscerà l'esito di una determinata profilazione, ad esempio il vedersi negare la possibilità di prendere un aereo, ma "non avrà alcuna possibilità di contestare i fatti alla base della decisione o la linea di ragionamento che ha portato a quel risultato" (Steinbock 2005, 8 traduzione dell'autore).

Se la posizione che il cittadino ha nei confronti dello Stato è uno degli indicatori della qualità di una democrazia liberale, l'uso di tecniche di profilazione da parte dello Stato mette seriamente in discussione questo fondamento. Questo non tanto rispetto al riconoscimento di alcuni diritti da parte dello Stato ma rispetto alla possibilità del cittadino di esprimere la sua personalità e partecipare attivamente alla vita democratica. Qui sta il valore fondamentale della autonomia e della autodeterminazione; valori che lo Stato non può garantire al cittadino semplicemente astenendosi dall'interferire nei suoi affari privati e personali (Rouvroy e Poullet 2009). Sebbene sia evidente quanto sia difficile garantire legalmente i valori di autonomia e autodeterminazione, creare le condizioni per la piena realizzazione delle libertà positive e negative e per il rispetto dell'autonomia individuale (Hildebrandt 2008b; Rouvroy e Poullet 2009) sono requisiti essenziali per una piena democrazia liberale.

In questo campo l'autodeterminazione acquista il particolare significato di autodeterminazione informativa, concetto che si deve a una nota pronuncia della Corte Costituzionale Tedesca del 1983[2].

L'autodeterminazione informativa implica che il singolo abbia il controllo dei suoi dati e delle informazioni che lo riguardano. La profilazione è per sua natura in tensione con questo principio. L'individuo non ha modo di sapere come i suoi dati saranno usati per elaborare dei profili e nemmeno se questi saranno applicati anche a lui:

> *the invisibility of the patterns that become visible to the profiler and the inability to anticipate the consequences of the application of*

[2] BVerfGE 65, 1 – Volkszählung Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983

profiles derived from other people's data clearly rule out informed consent (...) and the lack of information on how I am being categorised and what the consequences are turns the idea of self-determination into ridicule. (Hildebrandt 2009, 243)

Non essere consapevoli del perché si sta ricevendo una specifica proposta commerciale o determinate condizioni per il prestito del denaro limita lo sviluppo personale e l'attiva partecipazione: nel momento in cui non si sa cosa verrà elaborato dai dati che noi stessi rilasciamo spesso non consapevolmente, lo scambio di dati qualunque sia il vantaggio all'orizzonte non può essere considerato equo.

3.2 *La tensione con i diritti fondamentali*

Questi valori fondamentali sono strettamente correlati con il diritto alla privacy e alla protezione dei dati personali così come al diritto alla non discriminazione.

Come sottolineato da Rodotà,

the strong protection of personal data continues to be a 'necessary utopia' if one wishes to safeguard the democratic nature of our political systems. (Rodota 2009, 78)

Parimenti il diritto alla non discriminazione è l'essenza di una democrazia. Non per caso la Corte di Giustizia Europea, in due casi recenti in materia di profilazione[3] ha invocato sia la legislazione in materia di protezione dei dati personali che la normativa anti-discriminazione a fini di tutela dei diritti dei cittadini.

Senza soffermarsi sulle molteplici definizioni di privacy (Solove 2007) e sui rapporti con la protezione dei dati personali, ciò che interessa rilevare qui è che tanto la privacy quanto la protezione dei dati personali si presentano in tensione con le tecniche di elaborazione dati alla base della profilazione.

Si prenda ad esempio le informazioni conservate nelle RFID card

[3] Corte Europea di Giustizia, Huber v. Bundesrepublik Deutschland, C-524/06, 16 Dicembre 2008, http://curia.europa.eu/juris/liste.jsf?td=ALL&language=it&jur=C,T,F&num=C-524/06 Corte Europea di Giustizia, Test-Achats e altri v. Conseils des Ministres , C-236/09, 1 Marzo 2011, http://curia.europa.eu/juris/liste.jsf?td=ALL&language=it&jur=C,T,F&num=C-236/09

usate per il trasporto pubblico (come la Oyster e la Octopus card ampiamente usate a Londra e Hong Kong).

Queste carte contengono dati personali al fine di poter essere usati da una sola persona. L'elaborazione dei dati in esse contenute permette di delineare profili completi del viaggiatore e dei suoi consumi (visto che entrambe queste carte consentono anche l'acquisto di generi di consumo in alcuni negozi). Sebbene la persona abbia dato il consenso alla registrazione dei dati, non necessariamente immagina che da questi dati possono essere elaborati profili su abitudini di viaggio e di consumo di soggetti di una certa età, provenienza, condizione socio-economica. Profili che possono essere poi impiegati ad esempio a scopi di marketing. Inoltre i dati dei viaggiatori possono essere acquisiti dalle forze dell'ordine al fine di individuare schemi di spostamento sospetti. Nonostante i dati personali siano stati anonimizzati o comunque sottoposti a un processo di de-identificazione, non è impossibile che si applichi il processo inverso per re-identificare (Ohm 2010). L'opacità stessa del processo di profilazione sembra allontanare ogni possibilità di rendere trasparente l'uso dei dati raccolti.

Oltre al diritto alla privacy e alla protezione dei dati personali, anche il diritto alla non discriminazione è in tensione con le categorizzazioni su cui si basa la profilazione.

Il diritto alla non discriminazione è un principio guida della legislazione europea e di recente inserito come diritto fondamentale nell'articolo 21 della Carta Europea dei diritti fondamentali. Consta di un principio generale di uguaglianza (situazioni simili vanno trattate nello stesso modo e situazione diverse vanno trattate in modo diverso) e di specifiche divieti di discriminazione fondati su età, genere, razza, religione, orientamento sessuale in diversi campi di applicazione (p.e. il mercato del lavoro, il settore educativo o della salute, l'acceso ai servizi, etc.).

La distinzione di base nella normativa Europea (Direttiva 2000/43/EC), di grande rilevanza in materia di profilazione, è quella tra discriminazione diretta e indiretta, entrambe proibite. Come noto, si ha discriminazione diretta quando una persona è trattata in modo meno favorevole di un altra per ragioni legate al suo genere, età, razza, religione, orientamento sessuale. Si ha discriminazione indiretta quando criteri apparentemente neutrali hanno un effetto discriminatorio.

Tale distinzione è fondamentale in materia di profilazione perché raramente la categorizzazione operata dalle tecniche di profilazione si

base su uno dei criteri vietati dalla legge. Ma può accadere che gli algoritmi impiegati classifichino alcune caratteristiche che risultano essere una proxy dei criteri vietati. Il più chiaro esempio è la pratica del cd. *redlining*, proibito esclusivamente dalla legislazione statunitense. Si intende per *redlining* quella pratica di negare prodotti o servizi in determinati aree della città, tracciando una linea rossa su una mappa. Nelle città caratterizzate da una crescente segregazione abitativa o concentrazione demografica di persone aventi stessa classe sociale, condizione occupazionale o anche nazionalità, vivere in una determinata area della città significa ad esempio appartenere a uno specifico gruppo etnico. Ne consegue che un criterio apparentemente neutro come il codice postale nasconda una situazione di discriminazione.

Appare evidente che non è sufficiente prima di procedere all'elaborazione dei dati cancellare quelli sensibili, come chiaramente affermato da Romei e Ruggeri (2013, 121)

> *the naive approach of deleting attributes that denote protected groups from the original dataset does not prevent a classifier to indirectly learn discriminatory decisions, since other attributes strongly correlated with them could be used as a proxy by the model extraction algorithm.*

Non è quindi un caso se un numero crescente di studi si concentra su come prevenire la discriminazione nelle tecniche di data mining (in particolare si veda Custers et al., 2013).

4. Conclusioni

Democrazia, *rule of law*, autodeterminazione, uguaglianza possono essere messi a rischio dallo sviluppo tecnologico.

Le minacce a questi diritti e valori fondamentali sono tra loro collegate e si autoalimentano.

La profilazione sfida l'essenza della democrazia perché pone il ruolo degli essere umani in secondo piano nel processo decisionale e crea distribuzioni di potere ineguale e assimetria di conoscenza tra i cittadini da un lato e i governi dall'altro. Difficile risulta contestare le decisioni prese sulla base di tecniche di profilazione. Come si è visto il

diritto alla privacy, alla protezione dei dati personali e alla non discriminazione sono a rischio.

Allo stesso tempo però è innegabile che in quasi tutti i campi di applicazione rischi e benefici sono ugualmente presenti.

In alcuni di questi campi lo scontro tra gli interessi dello Stato o di soggetti privati (quali banche, assicurazioni ad esempio) e i diritti dei cittadini è evidente. In altri il quesito che emerge è fino a che punto i cittadini sono disponibili a permettere un maggior controllo? Sono disponibili a dare accesso a informazioni sensibili al fine di migliorare il servizio sanitario e ampliare la ricerca su nuovi campi ?

Difficile rispondere. Certamente la legislazione si trova oggi lontana dal fornire un adeguato livello di protezione. Il nuovo regolamento europeo sulla protezione dei dati va nella direzione di dosare il livello di protezione a seconda dello scopo del *data processing* e del livello di rischio. A prescindere dalla tipologia dei dati.

L'innovazione diretta a trovare soluzioni tecniche (c.d. *privacy by design*, *by default* e *value sensitive approach*) ai rischi di discriminazione e di attacchi alla privacy e alla protezione dei dati è certamente un'altra possibilità, sebbene ragioni di tempo, economiche e culturali – specie in alcuni Paesi – possono ostacolare l'effettiva implementazione di soluzioni tecniche nuove.

In ultimo una maggiore consapevolezza dei cittadini è certamente un tema fondamentale. Troppo spesso i cittadini acconsentono distrattamente alle richieste che vengono loro fatte on line o su formulari cartacei, ignorando che quei dati potranno essere usati per scopi commerciali, potranno essere ceduti a terzi, etc.

Certamente il rischio di un cittadino sempre più trasparente e uno Stato sempre più opaco aumenta, specie in occasione di eventi drammatici che riguardano la sicurezza dei cittadini. E ciò non renderà più sicuri e nemmeno liberi.

Valeria Ferraris
Dipartimento di Giurisprudenza – Università degli Studi di Torino
Lungo Dora Siena, 100
valeria.ferraris@unito.it

Riferimenti bibliografici

Anderson, Ben. 2010. "Preemption, Precaution, Preparedness: Anticipatory Action and Future Geographies." *Progress in Human Geography* 34: 777-798.

Bygrave, Lee Andrew. 2002. *Data Protection Law: Approaching its Rationale, Logic and Limits*. The Hague: Kluwer Law International.

Bosco, Francesca, Niklas Creemers, Valeria Ferraris, Daniel Guagnin, e Bert-Jaap Koops. 2015. "Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities." In *Reforming European Data Protection Law*, eds. Serge Gutwirth, Ronald Leenes, Paul de Hert. 3-33. Netherlands: Springer.

Canhoto, Ana Isabel, e James Backhouse. 2007. "Profiling under Condition of Ambiguity. An Application in the Financial Services Industry." *Journal of Retailing and Consumer Services* 14, 408-419.

Clarke, Roger. 1993. "Profiling: A Hidden Challenge to the Regulation of Data Surveillance." *Journal of Law and Information Science* 4: : 403-419.

Custers, Bart, et al. (eds.). 2013. *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*. Berlin: Springer.

Delsol, Rebekah, and Michael Shiner (eds.). 2015. *Stop and Search: The Anatomy of a Police Power*. London: Palgrave Macmillan

Fayyad, Usama M., Gregory Piatetsky-Shapiro, e Padhraic Smyth. 1996. "From Data Mining to Knowledge Discovery: an Overview." In *Advances in Knowledge Discovery and Data Mining*, eds. Fayyad Usama et. al. 1-34. Menlo Park (Cal.): American Association of Artificial Intelligence.

Giannotti, Fosca, e Dino Pedreschi. 2008. *Mobility, Data Mining and Privacy. Geographic Knowledge Discover*. Berlin, Heidelberg: Springer-Verlag.

Gutwirth, Serge, e Mireille Hildebrandt. 2010. "Some Caveats on Profiling." In *Data Protection in a Profiled World*, eds. Serge Gutwirth, Yves Poullet and Paul de Hert, 31-41. Dordrecht: Springer.

Hastie, Trevor, Robert Tibshirani, Jerome Friedman. 2009. *The Ele-*

ments of Statistical Learning. Data Mining, Inference, and Prediction. New York: Springer.

Hildebrandt, Mireille. 2006 "Profiling: from Data to Knowledge. The Challenges of a Crucial Technology." *DuD Datenschutz und Datensicherheit* 30: 548-552.

— 2008a. "Defining Profiling: a New Type of Knowledge?" In *Profiling the European Citizens. Cross-Disciplinary Perspectives*, eds. Mireille Hildebrandt and Serge Gutwirth, 17-47. Dordrecht: Springer.

— 2008b. "Profiling and the Rule of Law." *Identity in the Information Society* 1: 55-70.

— 2009 "Who is Profiling Who? Invisible Visibility." In *Reinventing Data Protection?*, eds. Serge Gutwirth, et al. 239-252. Dordrecht: Springer.

Marx, Gary, e Nancy Reichman. 1984. "Routinizing the Discovery of Secrets: Computers as Informants." *American Behavioral Scientist* 27: 423-452.

Ohm, Paul. 2010. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." *UCLA Law Review* 57: 1701-1776.

Rodotà, Stefano. 2009. "Data Protection as a Fundamental Right." In *Reinventing Data Protection?*, eds. Serge Gutwirth, et al. 77-82. Dordrecht: Springer.

Romei, Andrea, e Salvatore Ruggieri. 2013. "Discrimination Data Analysis: A Multi-disciplinary Bibliography." In *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, eds. Bart Custers, et al. 109-135. Berlin: Springer.

Rouvroy, Antoniette, e Yves Poullet. 2009. "The Right to Informational Self-Determination and the Value of Self-Development. Reassessing the Importance of Privacy for Democracy." In *Reinventing Data Protection?*, eds. Serge Gutwirth, et al., 45-76. Dordrecht: Springer.

Sanders, Carrie B., Crystal Weston, e Nicole Schott. 2015. "Police Innovations, 'Secrete Squirrels' and Accountability: Empirically Studying Intelligence Led-Policing in Canada." *British Journal of Criminology* 55: 711-729.

Solove, Daniel J. 2007. “I've Got Nothing to Hide’ and Other Misunderstandings of Privacy.” *San Diego Law Review* 44: 745 – 772.

Steinbock, D.J. 2005, “Data Matching, Data Mining and Due Process.”, *Georgia Law Review* 40: 1-84.

Van Brakel, Rosamunde, e Paul De Hert. 2011-2013. “Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategy.” *Cahiers Politiestudies* 20: 163-192.

Zakaria, Fareed. 1997. “The Rise of Illiberal Democracy.” In *Foreign Affairs* 76: 22-43.

Zarsky, Tal Z. 2002-2003 “‘Mine Your Own Business!’: Making The Case For The Implications Of The Data Mining Of Personal Information in the Forum of Public Opinion.” *Yale Journal of Law & Technology* 5: 1-56

— 2011. “Governmental Data Mining and its Alternatives.” *Penn State Law Review* 11: 285-330.